JURISGRADIBUS-*Articles* **ISSN: 2585-3554**

April-June, vol. 2, 2024 Article 2

TOWARDS PROTECTING VULNERABLE PEOPLE FROM THE NEVER-ENDING "CYBER WAR"

Luca Kavanagh
Doi:10.5281/zenodo.12759681

Doi:10.5281/zenodo.12759681

TOWARDS PROTECTING VULNERABLE PEOPLE FROM THE NEVER-ENDING "CYBER WAR"

Luca Kavanagh, Ph.D in international affairs, Legal adviser, US

Abstract: The aim of this work is to investigate yet another sector of vulnerability, i.e. of people such as children, women whose data is being exploited by a continuous "cyber war" that has been going on for many years without control despite the fact that the legislator of the European Union has tried since 2000 to frame the problem and lay the foundations for protection in the subject as still an important stage for the protection of fundamental rights. In our days a cooperation and collaboration with the European Convention of Human Rights and with some

decisions not so much from domestic level but from super partes to supranational courts have laid the interpretative foundations for the protection in this sector even going so far as to speak for protection and a continuous battle against modern terrorism.

Keywords: ECtHR; CJEU; ECHR; ICT; cybersecurity; vulnerability; cyberwarfare; fundamental rights; protection of human rights.

WHAT HUMAN RIGHTS VULNERABILITIES EXIST IN GLOBAL NETWORKS?

The technological path has made possible, in our times, to talk about the globalized right of vulnerability which includes the rights of children and women within a framework of fragility, weakness requiring a particular protection that respects the production risks between networks and beyond.

The concept of vulnerability cultivated by European law through jurisprudence has been augmented and aided by the European Court of Human Rights and by ad hoc European legislation as steps forward for particular protection (Cohet Cordey, 2000; Rouviere, 2010; Timmer, 2013; Paillet, Richard, 2014; Roux-Demare, 2019).

The vulnerability has to do with performance and application at various levels. Its use via information infrastructures is a never-ending reality. The European Union (EU) has talked about cyber security frequently as far as concern hard and soft law acts where the vulnerability of networks are part of a system that supports digital material towards, i.e. a cyber system at a global level.

In recent years we encounter the Strategy for Cyber Security in Europe (adopted in 2020); the so-called "NIS 2" Directive (n. 2022/2555)[1]; the DORA regulation 2022/2554 which was related to "digital operational resilience for the

[1]Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80-152.

financial sector"[2] and; Regulation 2021/784 on combating the spread of terrorist content online (Ahmed, 2023)[3]. Especially, the NIS 2 directive through Articles 6 and 15 put a particular note on the vulnerable right characterizing it as:

> "(...) a weakness, susceptibility or defect of ICT products or ICT services that can be exploited by a cyber threat (...)".

It is a fund that preserves the democratic order at the European level, as a legal space of freedom with a single market that is based on Article 114 TFEU and an an increased number of technical protection of networks thus identifying and eliminating the vulnerabilities they have a technical and present nature.

The relevant documents and guidelines are disseminated

[2]Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, PE/41/2022/INIT, OJ L 333, 27.12.2022, p. 1-79.

[3]Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. PE/19/2021/INIT, OJ L 172, 17.5.2021, p. 79-109.

by NATO as can be read in the latest manual entitled: “Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency” (Evans, 2022). It is a framework that expresses the vulnerability of networks and the reduction of rights with a proportional formula. Thus within the framework of attack both on a physical and geographical level a state should and seeks to police the same rights as an attack from a real enemy (Biçakci, 2022).

It is a process towards a particular cyber security strategy, within a global context of cyber warfare, which in recent years has done a particular job especially through the multilateral tensions that are growing, as we can see, in particular after the Russian-Ukrainian war and in Israel the last few months going on.

It is a race for internet networks where everyone writes and does what they want without any particular protection for those who misuse the internet[4]. War within a framework of digital revolution qualifies in an exhaustive legal way (Dennis, 2014) the cybernetic dimension which

[4]Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final of 16 December 2020.

has made it impossible to create a precise ad hoc definition. If the objective of protection and framework is missing, it is also difficult to legislate at a national level.
The forms of bellum within the digital environment are classic interstate conflicts that allow defense protected by international law to a different environment. In such a case, commercial and financial warfare as we have seen from the DORA[5] regulation is paralleled within the general protection of terrorism.
These are internal activities within a contrast where crime at a transnational level reports every contribution that trubles the proportion of a vulnerability of the networks which also has a positive impact on the protection of rights. A right towards a war where every global state should now have a cyber police as an exemplary paradigm for the protection of vulnerable people.

[5]See the Recital n. 1 of the DORA Regulation 2022/2554: "(...) growing degree of digitalisation and interconnection amplifies cyber risks, making the entire society, and in particular the financial system, more vulnerable to cyber threats or ICT disruptions. The ubiquitous use of ICT systems and high digitalisation and connectivity are today key features of the activities of Union financial entities (...)".

CYBER SPACE AND INTERNATIONAL LAW IN PARALLEL "TO THE BATTLE" WITH EUROPEAN LAW

The battles in the cyber sector are not a new phenomenon but there are no jus cogens rules, nor treaties or international conventions to deal with. As a soft law model we have cyber defense, the work that has always been done by NATO as well as every other defense firm in this sector.

Firstly, the Tallinn manual as a law of war respects the technological framework (Schmitt, 2017). It is a manual that has been going on since 2017 as a result of organizing, rationalizing the practice within NATO countries and beyond, as a basis for every state that has had similar problems[6].

[6]The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitalized World (25 November 2011): https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf; Strategy for Operating in Cyberspace. Department of Defense (July 2011): https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf;

Cyberspace security has had difficulties that respected the jus gentium framework in relation to hostile acts such as attacks on the integrity of networks, the interruption of IT services, as well as bodies of state that entail the related responsibility. These are difficulties which in practice make a complex development of international law of a treaty, customary nature, where even at a regional level acts of a binding nature have been adopted in the matter as has happened in the context of the EU.

On a parallel level with international law, the EU has already tried to extend the regulation to a single digital market with greater safeguards and protection since 2000, which is why we have seen the first directives, such as for example Directive 2002/21/EC which established the first comprehensive regulatory framework for electronic communications networks and services following after the Directive 2002/58/EC which dealt with personal data and for the first time privacy protection is concerned.

The European Council in 2004 called for the first time to

Canada's Cyber Security Strategy (2010): https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

focus on a Global Strategy for Critical Infrastructure putting Directive 2008/114/EC[7] into practice. Then, the EC Regulation n. 460/20042 established the Agency which was dedicated to network security[8]. It was based legally on art. 114 TFEU that established the functioning of the internal market.

The main objective of the above acts was cyber security as a precondition that brought economic exchanges to a single market. From 2008-2010 the commitment of the EU continued and took the European strategy at national level according to common guidelines.

We have seen in practice the EU Regulation n. 526/2013[9] which built on previous work and established ENISA, i.e.

[7]Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.

[8]Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1–11.

[9]Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58.

the European Union Agency for Network and Information Security as a new stage for coordination on information security and awareness for the strategic nature of economic development.

The multilevel of the Union was a basic step for the European Directive n. 2016/1148 (so-called "NIS" Directive, Network and Information Security)[10] which was intended to establish the common level of security of networks and information systems in the Union. It is an isolated act that has inserted a framework according to the European legislator for the strengthening and defense of the interests, networks and strategic assets for the Member States of the Union within a complex of basic acts that have opened, rectius matured the way to arrive at regulation 2019/881[11] which reinvigorated ENISA and created a

[10]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

[11]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity

cybersecurity certification system, thus replacing the regulation of 2013.

ENISA itself and the related acts have provided important guidelines for the collection of security cybernetics practices where the legislator of the Union followed the adaptation of European law to national law.

The coordination of supervisory powers, of sanctions, often of a mixed, certified and authorized nature has opened the way for new protection procedures for the near future. Identifying the sectoral authorities responsible for economic and social activities at an administrative level constitutes a technical network which is made up of the national CSIRTs, i.e. the relevant groups at European level for information security that also provided for by art. 9 of the NIS Directive.

Within this framework, the NIS 2 of 2022 Directive has further extended the scope of application of a regime of various private activities noting that it was created a European database for vulnerability according to art. 12.

As early as April 2023, the European Commission passed a new regulatory act, the Cyber Solidarity Act, which

Act). PE/86/2018/REV/1, OJ L 151, 7.6.2019, p. 15–69.

installed the European Cyber Shield and a Cyber Emergency Mechanism at European level as a model of help and support for interstate cooperation mechanisms in the sector[12], thus highlighting new legal bases where the relevant regulation was based on art. 173, letter. 3)TFEU which is dedicated to industrial policies within the Union (Blanke, Mangiamelli, 2021).

TOWARDS A MULTILEVEL PROTECTION OF DIGITAL RIGHTS AS A GREATER PROTECTION OF CYBERSECURITY

The protection of digital rights and of systems networks was an important job for the supranational legislator where the European Commission proposed, through the principle of solidarity, related legislation for the protection of various fundamental rights which are already provided for

[12]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM/2023/209 final, 18 April, 2023.

by the Nice Charter.
We are talking about rights that have to do with freedom and security, privacy and family life, freedom of enterprise and private property while also protecting public health care and the right to access services of economic interest general.
Cybersecurity is now a path towards a special wall that protects individuals and their rights in a collective security framework, i.e. as a guarantee of individual security that presents a community that strengthens individual rights at a transnational level.
The cyber space reproduces the same risk phenomena where cybersecurity measures monitor the mass and connection data paving thus the way for a European and not only control regime, an evaluation subordinated to the existence of guarantee of freedom of security dimension (Warusfel, 2021).
These are measures that are implemented not by public authorities but by private entities that have controlled technological infrastructures of communication without spatial limits and by rules that have highlighted the regulations as limits to fundamental rights in security and

defense, as procedures where states emergency situations require various constitutional bodies to interpret a principle that separates powers.
The framework of the cyber space is now a new reason for a supranational level that finds the relevant tools as a balance to the legitimate needs of the community such as security of enjoyment of rights and freedoms that follow both the domestic and Union law.

SUPPORT FROM THE COURT OF JUSTICE OF THE EUROPEAN UNION

The General Data Protection Regulation of 2016 (Liakopoulos, 2019)[13] no. 2016/679, was an important milestone for the regulation of big data as a collection of users by the continuous development in the profiling web.
A regulation that did not apply to issues that had to do with

[13]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (Regulation general on data protection), in the OJ, L 119/1 of 4 May 2016.

national security such as number no. 16 and 19. The protection of security in the cyber world made the private individuals who managed the infrastructures responsible and who physically respected the areas of application which guaranteed the security of the control and evaluation of the public authorities.
The regulation is also dedicated to the security of personal data after art. 32 following procedures that detected in a technical way the subjects who carried out the treatments.
Art. 33 dealt with data breaches such as theft of personal data which is committed through related hacking activities. The data controller communicated to the authority that he was responsible for the protection of personal data and the related investigations for the adoption of necessary countermeasures.
The relevant European legislative act was a possibility for the states that adopt the limits, obligations and rights foreseen by the relevant regulation.
This respected the fundamental rights within a democratic society that safeguarded the fundamental assets of a community of defense, national security and investigation of crimes as bases for the protection of rights which also

found support in the European Convention of the Human Rights (ECHR).
The GDPR, after the Directive 2002/58/EC, has dealt with personal data for the protection of privacy in the electronic communications sector as well as art. 13 of the directive 95/46/EC which was repealed after the regulation of 2016.
The restrictive measures through the CJEU ruled on security activities and criminal repression by states that protect personal data for users.
Within this framework and in occasion of the ruling of tele2 Sverige of 21 December 2016, the CJEU stated that:

> "(...) national legislation which, for the purposes of fighting crime, provides for generalized conservation and undifferentiated treatment of all traffic data and data relating to the location of all subscribers and registered users covering all means of electronic communication (...). It is not possible for states to regulate the protection and security of traffic data and location data, and in particular the access of the competent national authorities to the retained data, without limiting, in the context of the fight against crime, such access to the sole purpose of fighting serious crime, without subjecting such access to prior control by a judge or an independent administrative

> authority, and without requiring that such data be stored in the territory of the Union (...)"[14].

The protection of personal data and the balance of public security needs, was noted in the Schrems II case (Dhont, 2019; Chander, 2020; Christakis, 2020; Flett, Wilson, Clover, 2020; Tracol, 2020; Liss, Peloquin, Barnes, Bierer, 2021; Davis, 2023)[15]. This did not highlight the absence of physical borders that had to do with the application of the relevant cyberspace regulations as well as the relationships between the European, transnational legal space and the external one. Instead, these are acts of soft law, as for example we see from the European Parliament which since 2015 has asked for the control, evaluation, supervision of the world of technology within the instrument of freedom and as a

[14]CJE, joined cases: C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others of 21 December 2016, ECLI:EU:C:2016:970, published in the electronic Reports of the cases, par. 123.

[15]CJEU, CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, ECLI:EU:C:2015:650, published in the electronic Reports of the cases. C-311/18, Facebook Ireland and Schrems (Schrems II) of 16 July 2020, ECLI:EU:C:2020:559, not yet published.

means for the relative control over the powers and relations of individuals (Kanetake, 2019; Bromley, 2023)[16]. The Schrems II case was the basis for data transfer within the EU as well as to the USA due to the continuous development of social media such as Facebook, Instagram, Platform X, etc. Companies that evaded obligations and guarantees that found "their home" in the GDPR, as data transferred beyond the European context for the security and defense of human rights on a now global level but with many gaps to fill.

It was the same CJEU that denied the recognition of the applicability of the GDPR, where the agreement between the EU and the USA was now a wall of control for privacy, a regime that does not guarantee equivalent protection for the relevant regulation and access to the use of data by public authorities for national security matters, as its final objective for the good administration of justice and certainly for the related public interest.

[16]European Parliament resolution of 8 September 2015 on "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries" (2014/2232(INI)), OJ C 316, 22.9.2017, p. 40-50.

EUROPEAN CONVENTION OF HUMAN RIGHTS AND CYBERSECURITY

In the context of the ECHR, the rights relating to cybersecurity are referring to the protection of privacy and having to do with art. 8 ECHR as a subject of the various rulings from the ECtHR which had to do with global data interception and state security assurance.

In the Big Brother Watch v. United Kingdom and the Centrum För Rättvisa v. Sweden case of 25 May 2021 (Villiger, 2023) the ECtHR has set the guidelines for the right to privacy, the protection of public safety concerning the conduct of new technologies, developing thus the interceptions which have precisely sized the phenomenon in a general way and in absence of other specific targets against threats to state security. The ECtHR did not deny the international dynamics in the sector.

Moreover, an extensive analysis of the related data have ensured the internal, external security of the states believing that the domestic laws have framed the related

activities within an arbitrariness that has revealed the discriminatory and authoritarian acts.

The elements of each order were sufficient for the interceptions of boulders and compatible with what art. 8 ECHR pre-establishes. Elements that are framed in par. 361-362 of the Big Brother Watch case:

> "(...) -the reasons why it is possible to authorize a mass interception; -the circumstances in which an individual's communications can be intercepted; -the procedure to be followed to authorize such activities; -the procedures for selecting, examining and using intercepted material; -the duration limits of interception, of conservation of intercepted materials and the circumstances in which such material can be deleted or destroyed; -the procedures and methods of supervision by an independent authority on compliance with the previous elements and its sanctioning powers in case of violation; -the procedures for independent subsequent verification of this compliance and the powers vested in the competent body to deal with cases of violation (...)".

Instead, for personal data the police forces according to the P.N. v. Germany case of 11 June 2020 highlighted in a proportional way the relative conservation and processing

of personal data as prevention identification for crimes, especially serious ones, in order to avoid recidivism in the near future.

This is an increased level of protection where the application of cybersecurity measures have taken from criminal law.

It is also a general level of prevention towards a community with a specific way of threats where the preventive level involves control and electronic surveillance measures for certain identified individuals who do not commit crimes.

The canons of measures identified fall under the control of a third and impartial judge where the general measures are applied to the administrative authority in an erga omnes manner.

The cybernetic world thus becomes a complex that distinguishes general measures from the reality of subjects, specific groups that are outside the guarantees that are provided.

CYBER CONTROL, TERRORISM AND PROTECTION AGAINST EVERY CURRENT TERRORIST "WAR"

Cybersecurity also has another level of protection for one's rights which is part of the threats at the level of terrorism and especially for the maintenance of public order and the guarantee of human rights in the network.

The fight against terrorism, the balance for the poles and the demands that attract serious integrity risks for people are the basis of a general fear for the population, a phenomenon that defines the forms of regulation among those fighting European and international terrorism.

It is a context of protection where we already see in France through the French penal code to speak for terrorist websites where freedom of communication for internet users have the objective of canceling crimes even in a restrictive way.

The French Constitutional Council with the decisions n. 2016-611 QPC of 10 February 2017 and n. 2017- 682 QPC of 15 December 2017 (Goesel-Le Bihan, 2017; De Lamy, 2017; Latour, 2018; Hochmann, 2018; Catelan, 2018) has

considered that the relevant conciliation for the protection of public order and the prevention of crimes, freedom of information and related communication on the internet is above all instrumental in nature given the existence of possibilities for public authorities to combat the phenomenon of terrorism.

The judicial authorities implement the interception measures concerning electronic correspondence and images as well as the activities of collecting connection data with the related electronic correspondence and images as well as the collection of data and its connection with computer data.

Information services perform the acts of data control and the power of hosting providers to remove dangerous content. Thus the ordering as a general and preventive control tool makes restrictions on access to information collected from the internet.

The General Directive no. 2017/541 is a basis for the fight against terrorism which replaced the decisions of the Council having to do with criminal cooperation and the regulation dedicated to the fight against the contents of terrorist acts, information online which calls for greater

protection for cooperation between public and private for a just war.

Already in March of 2021 the Council approved the regulation to combat the spread of terrorist content online. In recital no. 1 it stated the followings:

> "(...) ensuring the smooth functioning of the digital single market in an open and democratic society by combating the misuse of hosting services for terrorist purposes and contributing to public security across the Union (...)".

The relative and immediate recipients are the states where, through the public authorities, private entities who have offered the information services requesting the contents from a supplier provide hosting services.

According to art. 3 the competent authorities for each state will have to directly direct and remove the hosting providers[17]. The transparency obligations, according to art.

[17]See for example the letter n° 2022-1159 of 16 August 2022 carrying different dispositions of adaptation to the right of the European Union in order to prevent the spread of terrorist-related content online. It is a law which has as its object the decision of the French constitutional council which was based on a prior basis to the relevant parliamentary minority. According to the decision n° 2022-841 DC of 13 August 2022 the Council took into consideration and accepted that the legislator did not violate the freedom of expression and communication as well as the injunctions that

7, had provided the relevant conditions of a contractual nature for the terms of a policy where the fight against terrorist content is subject to the sanctions provided for by art. 18 of the regulation.

This is an important point since it is part of a general form of partnership for protection objectives that established public strength and the guarantee of fundamental rights within the era of freedom, property, security and resistance to oppression, etc. These are important points that are also noted in all European democratic constitutions (Verpeaux, 2021)[18].

To define terrorism, in our days against the war in Ukraine, we use the European Parliament's resolution of 23

---

are issued by the administrative authorities and susceptible to appeal which was presented before the administrative judge according to the relevant emergency procedure of "référé-liberté" which was provided for in articles L. 521-1 and L. 521-2 of the French Code of Administrative Justice.

[18]See also from the French "Conseil constitutionnel" the decision n.2021-940 QPC of 15 October 2021 where it recognized the principle that is inherent to the French constitutional identity as a counter limit to European and international law which has to do with the ban on delegation of the public force and private entities.

November 2022. It is an important step for any future war in the sector even if not binding for the freedom of expression which puts all definitions in light.

CONCLUDING REMARKS

Arriving at some conclusions for the cyberspace in our times is a very difficult phenomenon given the continuous anarchy that goes on from the development of technology and the failure many times of states to conclusively follow every safeguard necessary for personal and of people data protection given that wars go on and change face even if the final result always remains the human victims.

General security for every state, in the European context and at a global level, is now a reality of the cyber dimension where the attempts at a balance sheet also from the jurisprudence of supranational and impartial courts do not arrive at ideal conclusions to satisfy the struggles in the sector that continue to go on ahead in time.

The problem many times is the disappearance of the relevant forms where continuous digitalism has to do with the rights procedure, the provision of obligations on

private individuals (Pollicino, De Gregorio, 2021) and not with protection for the community, since it is now an endless reality.

The most relevant forms are now missing. The procedures at a constitutional and public level are no longer solemn and the continuous effort of debate to avoid decisions for the protection of fundamental rights are now evolving ways where the principle of formal equality at a first ideological and then political level it involves the politics of a general will that applies to everyone.

The technical indications, the common sense of the decisions through the supranational courts place the judges in a continuous endless arbiter where many times the final sentence we do not know if it protects the life and democracy of an evolving state and/or human beings. Perhaps that will be the new challenge for the near future both at a European and international level.

REFERENCES

AA.VV. (2022). La QPC, outil efficace de protection des personnes en situation de vulnérabilité?. *Titre VII. Conseil Constitutionnele,* 52ss.

Ahmed, R. (2023). Negotiating fundamental rights: Civil society and the EU Regulation on addressing the dissemination of terrorist content online. *Studies in Conflict & Terrorism,* 1-25.

Biçakci, S. (2022). Cyber threats to critical infrastructure. In C.V. Evans, *Enabling NATO's Collective Defense: Critical infrastructure security and resiliency NATO.* COE-DAT Handbook 1. Carlisle Pennsylvania, 42ss.

Blanke, H.J., Mangiamelli, S. (2021). *Treaty on the Functioning of the European Union. A commentary,* ed. Springer, Berlin.

Bromley, M. (2023). The EU Dual-use Regulation, cyber-surveillance and human rights: the competing norms and organised hypocrisy of EU export controls. *Defence Studies, 23(4),* 644-664.

Carlier, J.Y. (2017). Des droits de l'homme vulnérable à la vulnérabilité des droits de l'homme, la fragilité des équilibres. *Revue Interdisciplinaire d'Études Juridiques, 220,* 3ss.

Catelan, N. (2018). Consultation de sites terroristes: quel dialogue entre le legislateur et ses juges?. *Revue Française de Droit Constitutionnel, 115,* 647ss.

Catherine, A., Etoa, S. (2020). Vulnerabilité et droit public. *Cahier des Recherches sur les Droits Fondamentaux, 18,* 2ss.

Chander, A. (2020). Is data localization a solution for Schrems II?. *Journal of International Economic Law, 23,* 772ss.

Christakis, T. (2020, July, 21). After Schrems II: Uncertainties on the legal basis for data transfers and constitutional implications for Europe. *Europeanlawblog.eu*: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/

Cohet Cordey, F. (eds.). (2000). *Vulnérabilité et droit. Le développement de la vulnérabilité et ses enjeux en droit*. Presses Universitaires de Caen. Grenoble.

Davis, M. (2023). Internet cookies in European Union (EU) law. *Juris Gradibus, 2(1),* 38-64.

De Lamy, B. (2017). La lutte contre le terrorisme à l'épreuve du contrôle de constitutionnalité: utiles précisions sur la nécessité d'une incrimination. *Revue de Science Criminelle et de Droit Pénal Comparé, 2,* 387ss.

Dennis, H. (2014). *Cyberwarfare and the laws of war.*

Cambridge University Press, Cambridge-New York.
Dhont, J.H. (2019). Schrems II. The EU adequacy regime in existential crisis?. *Maastricht Journal of European and Comparative Law, 5,* 598ss.
Evans, C.V. (eds). (2022). *Enabling NATO's collective defense: Critical infrastructure security and resiliency NATO.* COE-DAT Handbook 1. Carlisle Pennsylvania.
Flett, E., Wilson, J., Clover, J. (2020). Schrems strikes again: EU-US privacy Shield suffers same fate as its predecessor. *Computer and Telecommunication Law Review, 6,* 162ss.
Goesel-Le Bihan, V. (2017). Une grande décision: la décision n° 2016-611 QPC. *Actualité Juridique. Droit Administratif, 8,* 434ss.
Hochmann, T. (2018, January, 11). Consultation habituelle, censure habituelle (À propos de la décision QPC rendue le 15 décembre 2017 par le Conseil constitutionnel. *Jus Politicum Blog:*
https://blog.juspoliticum.com/2018/01/11/consultation-habituelle-censure-habituelle-a-propos-de-la-decision-qpc-rendue-le-15-decembre-2017-par-le-conseil-constitutionnel-par-thomas-hochmann/
Kanetake, M. (2019). The EU's dual-use export control and

human rights risks: the case of cyber surveillance technology. *Europe and the World: A Law Review, 3(1),* 2ss.
Latour, X. (2018). La lutte contre les sites djihadistes et la liberté de communication. *La Semaine Juridique. Administrations et Collectivités Territoriales, 7,* 39ss.
Liakopoulos, D. (2019). Regulation (EU) 2016/679 on the protection of personal data in light of the "Cambridge Analytica" affair. *E-Journal of Law. An indipendent law Journal, 5 (1),* 4ss.
Liss, J., Peloquin, D., Barnes, M., Bierer B.E. (2021). Demystifying Schrems II for the cross-border transfer of clinical research data. *Journal of Law and the Biosciences*, 8, (2).
Paillet, E., Richard, P. (eds.). (2014). *Effectivité des droits et vulnérabilité de la personne.* ed. Bruylant, Bruxelles.
Pollicino, O., De Gregorio, G. (2021). Constitutional law in the algorithmic society. In AA.VV., *Constitutional challenges in the algorithmic society.* Cambridge University Press, Cambridge, 21ss.

Roman, D. (2019). Vulnerabilité et droits fondamentaux. *Revue des Droits et Libertés Fondamentaux, 19,* 2ss.
Rouviere, F. (2010). *Le droit à l'épreuve de la vulnérabilité.* Études de Droit Français et de Droit Comparé. ed. Bruylant, Bruxelles.
Roux-Demare, F.X. (2019). La notion de vulnérabilité, approche juridique d'un concept polymorphe. *Cahiers de la Justice, 4,* 620ss.
Schmitt, M.N. (eds.). (2017). *Tallin manual on the international law applicable to cyber warfare.* Cambridge University Press, Cambridge-New York.
Timmer, A. (2013). Quiet revolution: vulnerability in the European Court of Human Rights. In M.A. Fineman, A. Grear (eds.). *Vulnerability. Reflections on a new ethical foundation for law and politics.* ed. Routledge, London, New York, 148ss.
Tracol, X. (2020). "Schrems II": The return of the privacy shield. *Computer Law & Security Review, 39,* pp. 4ss.
Verpeaux, M. (2021). Les résistances de la Constitution française. *La Semaine Juridique. Édition générale, 46,* 2101ss.
Villiger, M.E. (2023). *Handbook on the European Convention on Human Rights*. ed. Brill, Bruxelles.
Warusfel, B. (2021). La cyberdéfense, dimension numérique

de la sécurité nationale. In S.Y. Laurent (eds.). *Conflits, crimes et régulations dans le cyberespace*. ISTE Editions, London, 107ss.